UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,703	12/21/1999	XI WANG	D/99192	3974

7590 11/15/2005

NIXON PEABODY LLP
8180 GREENBORO DRIVE
SUITE 800
MCLEAN, VA 22102

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,703	WANG, XI	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 18-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 AND 18-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 and 18-33 have been examined and this Non-Final rejection is in response to the Request for Continuation Examination.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 31, 2005 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 4-7, 12-15, 19-21, 24-25, and 27-33 are rejected under 35 U.S.C. 102(e) as being anticipated over Wright, et al. (US 6,084,969).

As per claim 1:

Wright, Et Al. disclose a public, non-commutative method for encoding an original message to be passed to a recipient by way of a grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme; **[col.7, lines 4-5 and 64-65 and col.10, lines 4-8]**

generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to

said grantor, wherein said grantor's private key and said recipient's private key are combined, and the combination of the private keys is based on said public key encryption scheme and provides that it is computationally difficult to recover the recipient's private key from the public proxy key even with the knowledge of the grantor's private key; and **[col.5, lines 2-4]**

applying the public proxy key to transform the encrypted message into a transformed message **[col.4, line 66 – col.5, line 1]**, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information **[col.4, lines 65-66 and col.10, lines 3-6]** and wherein no clear-text document is revealed during the transformation. **[col.12, lines 55-56 and col.14, lines 65-67; where Wright discloses a straight through process of the encryption and the re-encryption process throughout the transformation of the encrypted document without any interruptions or descriptions of any clear-text document have been revealed. Therefore, no clear-text was reveal because it is inherent to not reveal any clear-text document during the transformation due to security reasons where the purpose is safeguarding the document from unintended or untrustworthy persons that does not have the proper key or information and is decryptable by the recipient using the proper information.]**

As per claim 4: See col.14, lines 17-20; discusses the receiving, generating, and applying steps are performed by the grantor.

As per claim 5: See col.12, lines 55-59; discussing the providing the transformed message to the recipient.

As per claim 6: See col.12, lines 4-7; discusses decrypting the transformed message using information selected from the private key corresponding to the recipient and any available public information.

As per claim 7: See col.12, lines 4-7; discusses decrypting the transformed message using information using the private key corresponding to the recipient.

As per claim 12: See col.11, lines 47-56; discussing the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

As per claim 13: See col.14, lines 17-20; discussing the applying step operates on the second portion of the encrypted message.

As per claim 14: See col.8, lines 37-55; discussing the original message is passed to a recipient through at least one additional intermediate grantor by repeating the generating and applying steps for each additional intermediate grantor.

As per claim 15:

Wright disclose a public, non-commutative method for encrypting an original message to be passed a recipient by way of a grantor, the method comprising the steps of:

obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme; **[col.7, lines 4-5 and 64-65 and col.10, lines 4-8]**

generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor, wherein said grantor's private key and said recipient's public key are combined, and the combination of said grantor's the private key and said recipient's public key is based on said public key encryption scheme; and **[col.5, lines 2-5 and col.7, lines 64-67]**

applying the public proxy key to transform the encrypted message, into a transformed message **[col.4, line 66 – col.5, line 1]**, wherein the transformed message is decryptable by the recipient **[col.4, lines 65-66 and col.10, lines 3-6]** using information selected from the private key corresponding to the recipient's public key and available public key information **[col.9, line 48 – col.10, line 8]** and wherein no clear-text document is revealed during the transformation. **[col.12, lines 55-56 and col.14, lines 65-67; where Wright discloses a straight through process of the encryption and the re-encryption process throughout**

the transformation of the encrypted document without any interruptions or descriptions of any clear-text document have been revealed. Therefore, no clear-text was reveal because it is inherent to not reveal any clear-text document during the transformation due to security reasons where the purpose is safeguarding the document from unintended or untrustworthy persons that does not have the proper key or information and is decryptable by the recipient using the proper information.]

As per claim 19: See col.12, lines 4-7; discussing the message is decryptable by the recipient using information selected from the private key corresponding to the recipient.

As per claim 20: See col.8, lines 37-55; discussing the original message is passed to a recipient through at least one additional intermediate grantor by repeating the transforming step for each additional intermediate grantor.

As per claim 21: See col.3, lines 28-33; discussing it is computationally difficult to recover the grantor's private key from the public proxy key.

As per claim 24: See col.14, lines 17-20; discussing the receiving, generating, and applying steps are performed by the grantor.

As per claim 25: See col.5, lines 46-48; discussing obtaining said recipient's private key by said grantor.

As per claim 27: See col.3, lines 28-33; discussing it is computationally difficult to recover the grantor's private key from the public proxy key.

As per claim 28: See col.10, lines 4-8; discussing public encryption scheme is a discrete-logarithm-based encryption scheme, wherein said combination of said private keys comprises using the modular difference of both private keys as an exponent in a modular exponentiation.

As per claim 29: See col.5, lines 46-48; discussing obtaining the recipient's private key by the grantor.

As per claim 30: See col.12, lines 62-65; discusses implementing the method with one or more hardware or software devices configured to perform the method.

As per claim 31: See col.6, lines 37-46 and col.12, lines 62-65; discusses implementing the method with one or more computer-readable instructions embedded on a computer-readable medium and configured to cause one or more computer processors to perform the method.

As per claim 32: See col.12, lines 62-65; discusses implementing the method with one or more hardware or software devices configured to perform the method.

As per claim 33: See col.6, lines 37-46 and col.12, lines 62-65; discusses implementing the method with one or more computer-readable instructions embedded on a computer-readable medium and configured to cause one or more computer processors to perform the method.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-3, 8-11, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright, et al. as applied to claims 1 and 15 above, and further in view of Mittra (US 5,748,736).

As per claim 2:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). However, Wright fails to include an ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages utilizing the ElGamal scheme wherein is well known in the art for supporting source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wright is to include the ElGamal encryption scheme

because digitally signing the messages supports authentication and sender non-repudiation.

As per claim 3:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). However, Wright fails to include an ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages utilizing the ElGamal scheme wherein is well known in the art for supporting source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wright is to include the ElGamal encryption scheme because digitally signing the messages supports authentication and sender non-repudiation.

As per claim 8: See Wright on col.7, lines 3-5 and col.11, lines 10-11 and 47-56; discusses the encrypted message comprises a first portion and a second portion, the first portion encoding a generator and a random key, and the second portion encoding the original message, the public key corresponding to the grantor, and the random key.

As per claim 9: See Wright on col.14, lines 17-20; discussing the applying step operates on the second portion of the encrypted message.

As per claim 10: See Wright on col.11, lines 47-56; discusses the encrypted message comprises a first portion and a second portion, the first portion encoding the original message, a generator, and a random key, and the second portion encoding the public key corresponding to the grantor and the random key.

As per claim 11: See Wright on col.14, lines 17-20; discussing the applying step operates on the second portion of the encrypted message.

As per claim 22:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). However, Wright fails to include an ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages utilizing the ElGamal scheme wherein is well known in the art for supporting source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wright is to include the ElGamal encryption scheme because digitally signing the messages supports authentication and sender non-repudiation.

As per claim 23:

Wright discloses a public- private encryption method wherein uses private keys and public keys for encryption and decryption (col.7, lines 59-65). However, Wright fails to include an ElGamal encryption scheme.

Mittra teaches decrypting the encrypted message and then re-encrypting the message along with digitally signing the messages. Mittra discloses that the procedures of digitally signing the messages utilizing the ElGamal scheme wherein is well known in the art for supporting source authentication and sender non-repudiation (col.10, line 62 thru col.11, line 3).

Therefore, it would have been obvious for a person of ordinary skill in the art to modify Wright is to include the ElGamal encryption scheme because digitally signing the messages supports authentication and sender non-repudiation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 18 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright, et al. (US 6,084,969), and in further view of Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition).

As per claim 18:

Wright disclose a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients comprising generating a session key based on a random number **[col.11, lines 46-50]** privately maintained by only the owner, including the encryptor **[col.9, lines 51-52]**, of the original document **[col.5, lines 2-4 and col.7, lines 10-11]**, encrypting the original document with the session key to create an encrypted document **[col.5, lines 21-22 and col.7, lines 12-13]**, generating a proxy key based on a public key **[col.10, lines 26-28 and col.11, line 11]** corresponding to the selected recipient, and **[col.11, lines 65-67 and col.14, lines 35-36]** However, Wright did not include the Cramer-Shoup encryption scheme.

The Irish Times disclosed in its article "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" a Cramer-Shoup encryption scheme **[paragraph 4]** where this encryption was developed by mathematicians from IBM and Swiss Federal Institute of Technology to have created an unbreakable protection for computer data **[paragraph 2]**. Cramer-Shoup method

thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text **[paragraph 6]**.

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Wright with Cramer-Shoup encryption scheme as taught by The Irish Times because this method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text.

As per claim 26:

Wright disclose a method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients comprising generating a session key based on a random number **[col.11, lines 46-50]** privately maintained by only the owner, including the encryptor **[col.9, lines 51-52]**, of the original document **[col.5, lines 2-4 and col.7, lines 10-11]**, encrypting the original document with the session key to create an encrypted document **[col.5, lines 21-22 and col.7, lines 12-13]**, generating a proxy key based on a public key **[col.10, lines 26-28 and col.11, line 11]** corresponding to the selected recipient, and **[col.11, lines 65-67 and col.14, lines 35-36]** However, Wright did not include the Cramer-Shoup encryption scheme.

The Irish Times disclosed in its article "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" a Cramer-Shoup encryption scheme **[paragraph 4]** where this encryption was developed by mathematicians from IBM and Swiss Federal Institute of Technology to have created an unbreakable protection for computer data **[paragraph 2]**. Cramer-Shoup method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text **[paragraph 6]**.

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Wright with Cramer-Shoup encryption scheme as taught by The Irish Times because this method thwarts attacks of decoding encrypted messages passing through the network with bogus messages by adding another series of calculations which ensure the server leaks no information when responding to the bogus text.

Response to Amendment

Wright discloses that there are no clear-text document is revealed during the transformation [col.12, lines 55-56 and col.14, lines 65-6] where Wright discloses a straight through process of the encryption and

the re-encryption process throughout the transformation of the encrypted document without any interruptions or descriptions of any clear-text document have been revealed. Therefore, no clear-text was reveal because it is inherent to not reveal any clear-text document during the transformation due to security reasons where the purpose is safeguarding the document from unintended or untrustworthy persons that does not have the proper key or information and is decryptable by the recipient using the proper information.

However, per argument's sake that Applicant points to the prior art failing to show that there are no clear-text being revealed during the transformation, the Examiner disagrees. Applicant broadly claims the method of encoding an original message from grantor to recipient wherein did not claim any limitations regarding the specifics of whom is "obtaining an encrypted message...according to a public key encryption" or whom is doing the generating of the public proxy key or whom is applying the public proxy key to transform the encrypted message into a transformed message. Hence, the argument of the prior art Wright's proxy server knowing the message is not persuasive because claims 1-33 fails to have this limitation.

Discussions pertaining to the key being used for encrypting the message is discussed on col.11, lines 46-51 and re-encrypting the message using the new key is discussed on col.12, lines 55-56.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100